

TECHNOLOGY BRIEF

Security Management from CA Technologies and PCI Compliance

how can security
management
technologies
help me with
PCI compliance?

we can



table of contents

executive summary

SECTION 1
Challenge **4**

SECTION 2
Solution **5**

SECTION 3
Benefits **15**

SECTION 4
CA Technologies advantage **15**

SECTION 5
Next steps **16**

executive summary

Challenge

PCI compliance has become a business requirement for any company involved in the processing of credit card information. It requires strong security controls over all systems and applications that process or store cardholder information. These controls serve to enforce access rights to all confidential information, and to identify and remediate areas of potential exposure of customer credit card information. PCI compliance requires robust security across a range of systems and applications.

Opportunity

Security Management from CA Technologies provides proven solutions for helping to achieve PCI compliance by helping to ensure the privacy of all confidential cardholder information, and by detecting and correcting areas of potential exposure. Additionally, these solutions provide control over access to your applications, systems, and data.

Benefits

Security Management solutions from CA Technologies enable you to create security controls to help achieve PCI compliance. Access to all cardholder information is controlled and audited, applications are protected against attacks, and areas of exposure risk are detected and remediated effectively. Security Management from CA Technologies is an excellent foundation for a comprehensive PCI compliance program.

Section 1: Challenge

Protection of confidential cardholder information

Introduction to PCI compliance

The Payment Card Industry (PCI) Data Security Standard (referred to hereafter as “PCI”) represents a collaboration between the leading credit card institutions, including, among others, Visa, MasterCard, American Express, and Discover. This standard was jointly created to help ensure consistency of security standards for these card issuers, and to assure cardholders that their account information was secure, regardless of where the card was used for payment. As part of this effort, the Cardholder Information Security Program (CISP) was created in order to monitor compliance to this standard.

The standard was formally adopted in December 2004, with initial compliance required by June 2005. Version 1.2 of the standard became effective on October 1, 2008. Although there are financial penalties that can be levied against any vendor or service provider who does not comply with these regulations, the most important penalty is the denial of the ability of the merchant or service provider to accept or process credit card transactions. Such a penalty could destroy their business.

Summary of the PCI requirements

The PCI standard does not mandate specific technology or products. Rather, it defines industry best practices for how credit card information should be handled, communicated, and stored in order to reduce the probability of unauthorized access to that information.

Many of the requirements of PCI relate to strengthening the security perimeter—preventing the “bad guys” from accessing any internal systems or data that contain cardholder information. However, a number of events, such as the CardSystems scandal, illustrate that it is often the insider who is the cause of a major security breach. Therefore, the PCI standard includes a number of requirements whose sole purpose is to limit the access of vendor or services organization employees to full customer credit card information. The number of employees who are permitted to see the full credit card number, for example, is strictly limited only to those individuals who clearly “need to know” this information.

There are six major categories of requirements in the standard, each of which has a small number of subcategories of requirements. The following table lists these categories and major requirements:

Category	Requirements
Build and maintain a secure network.	<ol style="list-style-type: none">1. Install and maintain a firewall configuration to protect data2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data.	<ol style="list-style-type: none">3. Protect stored data4. Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a vulnerability management program.	5. Use and regularly update antivirus software 6. Develop and maintain secure systems and applications
Implement strong access control measures.	7. Restrict access to data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly monitor and test networks.	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an information security policy.	12. Maintain a policy that addresses information security

Section 2: Solution

Achieving PCI compliance

PCI compliance involves a variety of requirements, all of which are focused on different areas of establishing a secure environment for the communication and handling of private cardholder information. Some of these requirements are purely process-related, but most can be either achieved or aided through the use of technology in addition to improved security processes.

The PCI requirements that can most effectively be addressed by CA Technologies security solutions (each first reference is in **Bold**) include the following:

Requirement #1: Install and maintain a firewall configuration to protect cardholder data

Summary of requirement: Firewall configuration standards must be established that define processes, procedures, and requirements for securing all network connections. Firewalls must be deployed that restrict connections between publicly accessible servers and any system component storing cardholder data.

CA TECHNOLOGIES SOLUTION CA Host-Based Intrusion Protection System (CA HIPS)

CA HIPS provides three key technologies: standalone firewall, IDS/IPS rules, and system security guards. These three technologies, alone or in combination, provide broad protection. These protections are applied via a set of rules and policies and provide the following capabilities:

- **Firewall** blocks or allows traffic into or out of the system
- **The Intrusion Detection (IDS)** rules block known threats, while **Intrusion Prevention (IPS)** rules provide behavioral protection that helps block zero-day attacks, essentially blocking the unknown
- **System Security Guards** protect the core system services such as the registry, system configuration, etc.

There are several ways CA HIPS can provide protection for cardholder information. It can block or allow traffic from the endpoint, and can set policy so that the cardholder data is locked down and no action can be taken. Or, it can lock down the data so that it can only be accessed under specific circumstances and at specific times.

Requirement #5: Use and regularly update antivirus software

Summary of requirement: Antivirus software must be running on all email and desktop systems, and must be regularly checked to help ensure that it is actively running and capable of generating audit logs.

CA TECHNOLOGIES SOLUTION CA Threat Manager

CA Threat Manager is a robust solution that combines the best-of-breed capabilities of CA Anti-Virus with the anti-spyware capabilities of the CA Anti-Spyware solution. This integrated solution combats a range of malware attacks, including viruses, worms, keyloggers, rootkits, etc., as well as identifying and removing spyware and adware attacks. Because these solutions are integrated, CA Threat Manager can also attack blended threats that combine aspects of different categories of these malware attacks.

Requirement #6: Develop and maintain secure systems and applications

Summary of requirement: All system components must have the latest vendor-supplied security patches, and there needs to be processes in place that help ensure that applications are free from vulnerabilities.

CA TECHNOLOGIES SOLUTION CA SiteMinder®

One key element of Section 6.5 of the PCI standard deals with the need to help ensure that all custom applications are based on secure coding guidelines so that vulnerabilities do not exist, and if they do, they cannot be exploited. This section deals with the need to code applications in a manner that eliminates vulnerabilities such as invalidated input, bad session management, cross-site scripting attacks, buffer overflows, and improper error handling, among others.

CA SiteMinder can provide important capabilities to help meet some of these requirements and mitigate others. In particular, CA SiteMinder provides secure access to custom applications so that only authorized users can access these applications. Specifically, CA SiteMinder can help protect custom application code in the following ways:

1. It filters URLs to block access attempts containing characters and character strings that may prove harmful to the application or its users. This reduces the risk of cross-site scripting attacks because ill-formed URLs cannot get through the CA SiteMinder agent protection. No application modification is required to gain these benefits when CA SiteMinder is used.
2. It provides a robust session management capability to help prevent user sessions from being hijacked by unauthorized users who are attempting to access the resources of another user.

3. It provides centralized configuration management, so that distributed (and therefore, less secure) configuration is eliminated. This capability not only enables improved application security, but helps reduce overall administrative effort, thereby increasing the administrative scalability for any application environment.

In summary, CA SiteMinder can help to prevent replay attacks, session hijacking, impersonation attempts, and protect Web applications. In this way, CA SiteMinder provides robust capabilities to enable secure applications to be developed and deployed more easily, so as to achieve compliance with this section of the PCI standard.

Requirement #7: Restrict access to data by business need-to-know

Summary of requirement: Access to systems, applications, and data (especially cardholder information) must be tightly restricted to only those individuals who have a clearly defined need to obtain this information.

CA TECHNOLOGIES SOLUTIONS CA Role & Compliance Manager, CA SiteMinder, CA Access Control, CA Identity Manager

Despite the fact that this section is one of the shortest of the entire PCI standard, it is very broad in its scope, and compliance may require the most effort of any requirement in the entire standard.

Section 7.1.1 is intended to ensure that privileged users are granted only the least privileges necessary to perform their job responsibilities. **CA Role & Compliance Manager** supports this objective by providing a centralized interface for administrators to browse user privileges and identify any improper assignments. It can also be used to establish identity compliance policies, such as segregation of duties, and automate entitlement certification processes to efficiently validate user privileges.

One implication of section 7 is that a role management mechanism needs to exist in order to effectively control access to protected resources based on the user's responsibilities. In particular, 7.1.2 states, "Assignment of privileges is based on individual personnel's job classification and function." CA Role & Compliance Manager's advanced analytics reduce the time and effort involved in developing an accurate role model while the solution supports the management of roles throughout their lifecycles.

Section 7.1.3 requires that management explicitly approve requests for access privileges, and that approval be granted by signature. CA Role & Compliance Manager supports automated workflow for signing off on privilege requests as well as access certification. Automating certification processes is essential to efficiently confirming that existing access privileges are appropriate, particularly accounting for cases where the standard provisioning process may have been bypassed.

Section 7 requires that all computing resources (that store or process credit card information) be available only to those people whose job requires such access. The term "resources" needs to be viewed in its full generality, and solutions and processes must include protection of all of these resources in order to achieve compliance. Specifically, access to Web applications, enterprise applications, host systems, databases, system files, critical system services, and even "superuser" access rights needs to be tightly controlled. Any solution that does not provide protection for these resources is not sufficient to meet the intent of this requirement.

CA SiteMinder is an industry-leading solution for Web application access management. Specific policies can be easily defined that will help ensure that only appropriate individuals will be able to access the applications and confidential information related to credit card processing. In addition, by centrally enforcing all access to these applications, development and maintenance of Web applications generally becomes simpler because application developers can focus on the business logic of the application rather than on enforcing security within each application.

Access to any host systems that process credit card information must also be tightly controlled. Users who are not authorized to view confidential cardholder information should not be allowed access of any kind to the systems that house that information. To protect against malicious acts against those systems, critical system files and even the rights to control or terminate critical system services must be strongly enforced.

Protection of the servers that host credit card information or related applications is particularly challenging in regards to privileged users (IT and Security Administrators). Whether inadvertent or malicious, improper actions by privileged users can have disastrous effects on IT operations, and on the overall security and privacy of corporate assets and information. Therefore, it is essential that privileged users be allowed to perform only those actions that are required for their specific responsibilities, and only on the appropriate assets.

CA Access Control is a leading solution for privileged user management that controls access to host systems and critical data and files residing on these systems. Policies can be defined that help ensure that only properly authorized users can gain access to each such system or resource. In this way, CA Access Control extends the basic security capabilities supported by each native operating system and provides an expanded, consistent, and more granular set of security capabilities across the systems in your environment.

Regardless of the methods used to control access to this cardholder information, a robust infrastructure for managing user entitlements is required. A centralized identity administration solution is required in order to help ensure that all user accounts and access rights are correctly established, and fully auditable. **CA Identity Manager** is a robust solution that provides an integrated identity management platform that helps automate the creation, modification, and suspension of users' identities and their access to enterprise resources to increase security levels and compliance. In addition, CA Identity Manager provides auditing services that can be used by both internal and external auditors to help determine if the organization's entitlement-granting practices are in control and effectively keeping private cardholder data private.

These four solutions are key elements of the overall solution for identity and access management from CA Technologies. These solutions provide identity administration and provisioning, role management and identity certification, and access management for all types of resources.

Requirement #8: Assign a unique ID to each person with computer access

Summary of requirement: All actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

This long section of the standard includes a number of specific security requirements. These can be summarized as follows:

- Identify all users with a unique username
- Use a variety of authentication methods, based on the sensitivity of the application or information being accessed
- Use two-factor authentication for remote access to the network
- Ensure that strong password policies exist and are followed
- Implement access restrictions based on failed access attempts as well as periods of user inactivity
- Immediately revoke access for any terminated users
- Remove/disable inactive user accounts at least every 90 days

CA TECHNOLOGIES SOLUTION CA Identity and Access Management, Privileged User Password Management (PUPM), CA UNIX Authentication Broker, Arcot WebFort, Arcot RiskFort

The **CA IAM** solutions provide all of these capabilities. As an example, CA SiteMinder supports a broad range of authentication methods so that the strength of the method can be associated with the sensitivity of the information or application being accessed. So, virtually any authentication methods can be combined to provide two-factor authentication for remote users.

In addition, **CA Identity Manager** provides flexible and robust capabilities for managing and controlling user passwords. Specific policies can be enforced that determine the length, format, and frequency of change, and even the content of the passwords. Passwords can be as arbitrarily strong as the needs of each IT environment dictate, thereby satisfying the requirements of this section of the standard.

In addition, Identity Manager provides automated deprovisioning of user access so that terminated users' access privileges can be removed immediately, and their associated accounts can be terminated.

CA Role and Compliance Manager can be used to identify orphaned accounts, which are accounts for users that are no longer in the system. This helps close an important security vulnerability that exists in most enterprises.

A common problem in many IT environments relates to the use of shared passwords among privileged users (administrators, root users). When administrators share their system and account passwords, it results in two very important problems. First, users of these shared passwords essentially become anonymous, and their actions cannot be associated with the person who performed them should an audit be necessary. Second, it usually results in "overprivileged" users, since they may be granted entitlements that they don't need to perform their normal job function.

What is needed, both for better security and PCI compliance, is a more secure way of allocating privileged user passwords. CA Access Control includes **Privileged User Password Management (PUPM)**, a capability that helps provide accountability of privileged access through the issuance of passwords on a temporary, one-time use basis. Once the password is used, it is no longer valid and therefore cannot be shared with other administrators. In addition, PUPM provides accountability of administrator actions through secure auditing, so that all administrator actions can be associated with a single individual (as required by this section of the standard).

There is another potential problem related to authentication of users that could hinder compliance with PCI. Authenticating UNIX/Linux users typically means maintaining records separate from Windows users. This complicates password synchronization, and can introduce delays in deprovisioning users. **CA Access Control Premium Edition** includes the **UNIX Authentication Broker (UNAB)**, a component that enables the management of UNIX users in a single user store, Windows Active Directory (AD). This provides consolidation of authentication and account information into one enterprise AD directory instead of maintaining credentials on various UNIX/Linux systems. This should help centralize and strengthen your authentication capabilities, thereby improving your PCI compliance profile.

One of the most important requirements of this section relates to strong, multi-factor authentication. Although there are many specific requirements in this section, many of them can be summarized as “deploy, effective 2-factor authentication”. Although important for high-value transactions or for certain remote users, many companies have resisted this due to perceived inconvenience of using and managing 2-factor tokens.

Arcot WebFort is a software-only multi-factor authentication solution that eliminates these problems and provides increased security to meet this PCI requirement. It is integrated with CA SiteMinder so that it transparently protects and verifies Web users’ identities. It protects users from identity theft and fraud without changing their familiar sign-on experience, nor requiring the possession of hardware tokens. It also eliminates the management effort and cost associated with hardware tokens.

WebFort uses ArcotID, a secure software credential that hides sophisticated two-factor authentication from your users. It leverages the user’s mobile phone as a factor of authentication through the generation of a one-time password or the receipt of a one-time password via an SMS text message. It appears to the user as the standard name/password sign-on, but it actually uses public-key infrastructure based challenge/response to verify the user’s identity before granting access to SiteMinder-protected applications. In this way, it protects you from man-in-the-middle, phishing, pharming, password cracking and brute force attacks. The combination of CA SiteMinder and CA WebFort therefore provide an excellent way to meet many of the requirements of this section of the standard.

Arcot RiskFort is a fraud detection and risk-based security system that prevents fraud in both consumer and enterprise online services. It also provides organizations the ability to determine and enforce different levels of authentication based on the acceptable amount of risk for the given transaction. Based on a risk score and company policies, organizations can enforce other forms of strong authentication, including the use of WebFort, depending on the user and the type of desired transaction. RiskFort can be deployed on the customer's premise or be consumed from the cloud as a cloud security service.

The combination of WebFort and RiskFort, in conjunction with the extensive authentication capabilities of CA SiteMinder, provide extremely flexible and strong authentication for all users.

Requirement #10: Track and monitor all access to network resources and cardholder data

Summary of requirement Logging mechanisms and the ability to track user activities are critical. Full logging of user and administrative activity is essential for tracking and analysis of all security events.

This section includes a number of very specific requirements. These can be summarized as follows:

- Establish a process for linking all access to system components (especially those done with administrative privilege, such as root) to an individual user
- Implement automated audit trails
- Record all important security events within the environment
- Secure audit trails so that they cannot be altered
- Review logs for all system components at least daily
- Retain the audit trail history for a period that is consistent with its effective use

CA TECHNOLOGIES SOLUTION CA Enterprise Log Manager (CA ELM)

CA ELM provides all of these capabilities—helping organizations simplify IT activity compliance reporting and investigations. It collects, normalizes, and archives IT activity logs from multiple sources and provides search, analysis, and reporting capabilities that can significantly reduce the cost and complexity of proving PCI compliance. It comes with hundreds of queries and reports available right out of the box. As an example, using these preconfigured queries and reports that are mapped to PCI, you can identify and investigate “SA,” “root,” or any default administrator account activity which is in clear violation of PCI requirement 10.2. You can even set up automated alerts if such violations happen in the future. It provides a secure and reliable collection and transport of logs, while providing role-based access to IT activity data in order to mitigate the risk from unauthorized access and modification.

With CA ELM's Web-based dashboard delivering multidimensional and visual log analysis tools, the time needed to conduct daily review of logs can be significantly reduced, and the process for determining violations of defined controls can be made more efficient. Finally, CA ELM provides both online (short-term) and offline (long-term) log storage options, which are critical in demonstrating compliance with requirements that auditable records must be retained for an extended period of time. In addition, CA ELM is designed to efficiently compress logs by a 10:1 ratio, thus helping reduce log storage costs.

Data Loss Prevention for more effective PCI compliance

Data Loss Prevention (DLP) can significantly strengthen the controls that help ensure the protection of customer credit card information. The benefits of DLP span the PCI requirement categories, so this section will summarize its benefits across several of these categories.

The CA DLP solution (CA DLP) provides two critical capabilities for use in PCI compliance programs:

1. Detection of unprotected PCI-relevant data.

CA DLP can scan an enterprise for data such as credit card numbers, account holders' personal information, and the like. If it is found in a location that doesn't have sufficient protections required for this kind of data, CA DLP can move the data to a secure location, and can delete the original file. This protects an organization from rogue "backup" copies of production customer data that may make their way to an improper place. This helps an organization ASSESS its own enterprise for possible vulnerabilities, as well as REMEDIATE risks by taking action on unprotected data across the enterprise.

2. Detection of this unprotected data in motion or in use throughout the enterprise.

In the case where an employee gets access to data that should be protected, CA DLP can help to meet PCI requirements by detecting and preventing the movement of that data. This can occur at the network boundary in many forms—such as in email (SMTP), FTP, HTTP, IM, Webmail, and many more network protocols. This can also occur on endpoint assets (such as a laptop or a workstation) where an end user is attempting to move PCI-protected data to removable media (such as a USB thumb drive) or is trying to print the data. CA DLP can help protect the data that requires protection as per the PCI mandates by blocking it from being moved to portable media or to a location external to the firm. CA DLP also provides robust reports on all risks that it detects, and all actions that it takes. Data can also be sent to log management solutions, like CA ELM, for centralized reporting.

CA DLP offers several prebuilt policies to detect “cardholder data,” such as:

Credit Card Numbers	Protect and control credit card numbers in various ranges and formats.
Credit Card Numbers—Threshold	Protect and control a specified amount (or threshold) of credit card numbers in various ranges and formats.
Credit Card Numbers with additional PII	Protect and control credit card numbers when accompanied by additional identity information, namely address, DOB, and name.
Sharing of Passwords and Usernames	Protect and control the disclosure and sharing of passwords, and prevent the distribution of user names or passwords in an unsecured format.

In summary, CA DLP is an important component in enabling a firm to adhere to PCI standards by ASSESSING their vulnerabilities, REMEDIATING them (in real time), and REPORTING on them.

PCI Compliance for the Mainframe

Any comprehensive strategy for PCI compliance needs to incorporate mainframes, due to their critical nature in any security environment. In particular, some previous very public breaches of customer credit card information involved inadequate mainframe security. CA Technologies offers a number of mainframe security solutions that can enable you to incorporate mainframes into your PCI compliance strategy, along with the other CA distributed security solutions. The CA Mainframe security solutions include:

- **CA ACF2™ and CA Top Secret®** provide flexible and robust capabilities for managing identities and entitlements. Specific policies can be enforced to determine the length, format and complexity of passwords. Life of user passwords can also be controlled on both a global or individual basis. Password strengths can be managed by an organization; given their specific IT environments. CA ACF2 and CA Top Secret help you meet several of the PCI requirements, most importantly sections 7.1.4, 7.2.1, 7.2.3, 8.1, and 8.5.8, 9.10.2.
- **CA ACF2™ and CA Top Secret® Option for DB2** allows you to control the security of your critical DB2 for z/OS environment where it’s most practical: within the existing CA ACF2 or CA Top Secret access control system and helps you meet several of the PCI requirements, including 6.2, 6.3.6, 7.1.4, 7.2.1, 8.1, 8.5.8, 10.1, 10.2, 10.2.1, 12.5 and 12.5.5.
- **CA Auditor for z/OS** helps identify the system, application and security exposures in z/OS environments that arise from improper system configuration and operational errors, as well as intentional circumvention of controls and malicious attacks. This solution helps you meet the PCI requirements for sections 6.2, 6.4, 10.5.2 and 11.5.

- **CA Cleanup** provides mainframe identity and entitlement monitoring for your CA ACF2, CA Top Secret and/or IBM RACF security on z/OS. Specific policies can be defined to monitor the usage (or lack of usage) for identities and entitlements and after a defined period of inactivity, the entitlement and/or identity can be archived and then removed from the system. This prevents orphaned identities and entitlements from having the potential from causing adverse effects to PCI data. CA Cleanup can reduce unused permissions and user IDs without the high cost of manual administration. This solution helps you meet the requirements of PCI sections 2.1, 7, 8.5.5, 8.5.6, and 10.
- **CA Compliance Manager for z/OS** allows all activity against PCI (and non-PCI) data to be monitored in an effort to determine and maintain least-privileged access by all users who require access to PCI data to perform their job function. Also, CA Compliance Manager will assist in achieving and maintaining the least privileged access model. This will help ensure that the level of access a user has to an object, is the absolute access in which they require to perform their job. This solution helps you meet the PCI requirements for sections 6.4, 7, 10.2, 10.3, 10.5.2, 10.5.5 and 11.5.

Full details on how these solutions enable mainframe PCI compliance can be found at:
ca.com/mainframe/pci

Summary

Compliance with the requirements of the PCI standard has become a business imperative for firms that process significant numbers of credit card transactions, or provide any type of credit card services to other organizations. Although these requirements are based on industry best practices, it is unlikely that most organizations would initially comply with this standard without improvements in their IT security processes and system, as well as in their business processes.

Compliance with PCI requires a concerted effort, typically involving multiple groups within the IT organization. Although changes to various IT processes are usually involved, the adoption of specific technology solutions can greatly aid the compliance effort. CA Technologies offers solutions that not only protect assets and information related to cardholders, but can also help reduce overall IT costs by automation of many IT processes related to the protection of this information.

Section 3: Benefits

Security Management solutions from CA Technologies provide a proven solution for protecting your IT assets across the platforms and environments within your enterprise. These solutions can deliver the following key benefits:

Enabling PCI compliance Help provide your organization with the automated and centrally managed compliance capabilities that help to reduce costs, while providing strong controls and proof of controls that can strengthen security and improve IT auditing.

Reducing administrative costs and improving efficiency Reduce your security administration and help desk costs, as well as improve the overall productivity of your user population. By centralizing the management of all user identities and their access rights, management of your policies becomes easier, less error-prone, and significantly less costly.

Reducing security risks With centralized access rights enforcement, Security Management solutions from CA Technologies help ensure that only properly authorized users gain appropriate access to your critical resources. Users are entitled by their role in your organization, and receive only the appropriate levels of access to protected resources and/or other non-IT resources to perform their job functions. They also reduce the possibility of expired identities remaining active in your system. When an employee leaves your organization, access can be immediately revoked or completely removed from all points of access. In addition, preexisting unused (“orphan”) system accounts and access rights can be automatically detected and removed.

Improving business enablement Automating, centralizing, and improving control over security functions helps organizations to better secure their online applications and deliver more well-tailored and positive online user experiences to their growing ecosystem of employees, customers, suppliers, and business partners.

Section 4: CA Technologies advantage

Security Management from CA Technologies offers a unique combination of advantages, including broad reach across applications, platforms, and services; modular design based on common services and user interfaces; centralized and automated provisioning, workflow, and entitlement; and global scalability. These capabilities can make it easier to create a comprehensive PCI compliance solution for your environment.

Add value with CA Services An important part of CA Technologies' leadership in the security management market involves the dedicated CA Services identity and access management (IAM) practice team. Our security specialists understand your unique requirements, appreciate your risk profile, and can help you meet your business drivers and regulatory requirements. Working in partnership with you, CA Technologies can help you build a security infrastructure and implement a foundation of well-defined IT processes and controls. In designing your IAM solution, CA Services relies on blueprints based on the CA IAM Maturity Model, which incorporates our extensive security expertise and industry standards. Each blueprint plots the way to a progressively higher level of IAM maturity, delivering ROI-documented improvements to people, processes, and technology.

Section 5: Next steps

If you're finding that:

- PCI compliance is a requirement for your business
- You need to automate your key security and compliance processes
- You want a security management solution that's tightly integrated with your overall IT management approach

then take a look at Security Management solutions from CA Technologies, a market-leading and integrated security management solution addressing security for Web applications, legacy systems, distributed computing environments, and Web services.

For more information on how CA Content-Aware IAM can help you reduce security costs, protect corporate assets, and help ensure regulatory compliance through a more integrated and comprehensive security solution, visit us at ca.com/iam.

Copyright ©2010 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies. This document is for your informational purposes only. CA assumes no responsibility for the accuracy or completeness of the information. To the extent permitted by applicable law, CA provides this document "As Is" without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or noninfringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, business interruption, goodwill, or lost data, even if CA is expressly advised in advance of the possibility of such damages.

CA does not provide legal advice. Neither this document nor any CA software product referenced herein shall serve as a substitute for your compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, policy, standard, guideline, measure, requirement, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. You should consult with competent legal counsel regarding any Laws referenced herein.